

MIMO Wiretap Channel under Receiver Side Power Constraints with Applications to Wireless Power Transfer and Cognitive Radio

Karim Banawan Sennur Ulukus

Abstract

We consider the multiple-input multiple-output (MIMO) wiretap channel under a minimum receiver-side power constraint in addition to the usual maximum transmitter-side power constraint. This problem is motivated by energy harvesting communications with wireless energy transfer, where an added goal is to deliver a minimum amount of energy to a receiver in addition to delivering secure data to another receiver. In this paper, we characterize the exact secrecy capacity of the MIMO wiretap channel under transmitter and receiver-side power constraints. We first show that solving this problem is equivalent to solving the secrecy capacity of the wiretap channel under a *double-sided correlation matrix* constraint on the channel input. We show the converse by extending the channel enhancement technique to our case. We present two achievable schemes that achieve the secrecy capacity: the first achievable scheme uses a Gaussian codebook with a fixed mean, and the second achievable scheme uses artificial noise (or cooperative jamming) together with a Gaussian codebook. The role of the mean or the artificial noise is to enable energy transfer without sacrificing from the secure rate. This is the first instance of a channel model where either the use of a mean signal or the use of channel prefixing via artificial noise is *strictly necessary* for the MIMO wiretap channel. We then extend our work to consider a maximum receiver-side power constraint instead of a minimum receiver-side power constraint. This problem is motivated by cognitive radio applications, where an added goal is to decrease the received signal energy (interference temperature) at a receiver. We further extend our results to: requiring receiver-side power constraints at both receivers; considering secrecy constraints at both receivers to study broadcast channels with confidential messages; and removing the secrecy constraints to study the classical broadcast channel.

I. INTRODUCTION

Most existing literature on Gaussian channels is based on a transmitter-side average power constraint. This constraint models the *maximum* allowable power at the transmitter-side. Gastpar

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mails: kbanawan@umd.edu; ulukus@umd.edu). This work was supported by NSF Grants CNS 13-14733, CCF 14-22111 and CCF 14-22129, and was presented in part at the Allerton conference, Monticello, IL, October 2014.

[1] was the first to consider a receiver-side power constraint. In [1], he considered a *maximum* receiver-side power constraint motivated by the desire to limit the received interference in a cognitive radio application. He observed that, while the solution does not change with respect to a classical transmitter-side power constraint for a single-input single-output (SISO) channel, it changes significantly for a multiple-input multiple-output (MIMO) channel. Subsequently, Varshney [2] considered a *minimum* receiver-side power constraint motivated by the desire to transport both information and energy simultaneously over a wireless channel. This *minimum* receiver-side power constraint signified the power (in addition to data) transferred to the receiver by the same physical signal. Varshney as well observed that while the solution does not change with respect to a classical transmitter-side power constrained SISO channel, it changes significantly with respect to a classical transmitter-side amplitude constrained SISO channel [3].

In this paper, we consider a multi-user and multi-objective version of the problem considered by Gastpar and Varshney. In particular, we consider a MIMO wiretap channel where the transmitter wishes to have secure communication with a legitimate receiver in the presence of an eavesdropper. In this model, messages need to be sent at the highest reliable rate to the legitimate receiver with perfect secrecy from the eavesdropper. We impose the usual transmitter-side power constraint in addition to a receiver-side power constraint. Therefore, our model generalizes the receiver-side power constraint of Gastpar and Varshney from a single-user setting of two nodes to a multi-user scenario of a wiretap channel with three nodes, and also to a multi-objective setting where we have both reliability and security constraints.

The wiretap channel was first considered by Wyner in [4], where he determined the rate-equivocation region of a degraded wiretap channel. This model was generalized to arbitrary, not necessarily degraded, channels by Csiszar and Korner in [5], where they determined the rate-equivocation region of the most general wiretap channel. The SISO Gaussian wiretap channel, which is degraded, was considered under a transmitter-side power constraint in [6], which showed that Gaussian signalling is optimal. The MIMO Gaussian wiretap channel was considered in [7]–[9], under a transmitter-side power constraint. These references showed that channel prefixing is not needed, even though the MIMO wiretap channel is not degraded, and Gaussian signalling is optimal. An interesting alternative proof is given in [10] based on the *channel enhancement* technique developed in [11]. Reference [10] considers the MIMO wiretap channel under a

transmitter-side *correlation matrix constraint* which is more general than a transmitter-side power constraint. The results in [7]–[10] imply that artificial noise [12] or cooperative jamming [13] is not needed for a MIMO wiretap channel under a transmitter-side power constraint.¹

In this paper, we first characterize the secrecy capacity of the general MIMO wiretap channel under a *minimum* receiver-side power constraint at the eavesdropper only. To this end, we first show that, solving the secrecy capacity of the MIMO wiretap channel under a transmitter-side *maximum* power constraint and a receiver-side *minimum* power constraint is equivalent to solving the secrecy capacity of a MIMO wiretap channel under a *double-sided correlation matrix* constraint on the channel input at the transmitter. This is a generalization of the approach of [10], [11], which shows that solving the capacity under a transmitter-side *maximum* power constraint is equivalent to solving the capacity under a transmitter-side *maximum* correlation matrix constraint. We then generalize the channel enhancement technique of [10], [11] to the case of *double-sided* correlation matrix constraint. This gives us the converse.

We next show that the rates given in the converse can be achieved by two different achievable schemes: a *mean* based scheme where the transmitter uses a Gaussian codebook with a fixed mean, and an *artificial noise* [12] (or cooperative jamming [13]) based scheme, which uses Gaussian channel prefixing with a Gaussian codebook. The role of the mean or the artificial noise is to enable energy transfer without sacrificing from the secure rate; this helps to achieve the receiver-side power constraint by sending non-message carrying signals. This is the first instance of a channel model where either the use of a mean signal or the use of channel prefixing via artificial noise is *strictly necessary* for the canonical MIMO wiretap channel. Note that while [20, Section III] shows an alternative way of achieving MIMO secrecy capacity using artificial noise, this is valid in the case of a covariance constraint, and the use of artificial noise in the MIMO wiretap channel under a transmitter-side power constraint is strictly sub-optimal. We note that, in a related work, references [21], [22] consider simultaneous information and energy transfer in a MISO wiretap channel, and focus on optimizing the performance of a specific artificial noise based achievable scheme with no claim of optimality. We also note a similar set-up in [23], [24], where the authors consider the case of statistical channel state information only at the transmitter and focus on optimizing asymptotic transmit covariance matrix of Gaussian codebooks without

¹Note, however, that they may be needed in SISO/MISO/MIMO wiretap channels with imperfect channel state information (CSI) [14]–[18] or multi-user versions of the wiretap channel (e.g., multiple access) even with perfect CSI [13], [19].

artificial noise for the case of a large number of transmit antennas.

We then extend the developed methodology to find the capacities of the following related channels. We first consider the case that both receivers (both Bob and Eve) have *minimum* receiver-side power constraints. This corresponds to the case where wireless power should be delivered to both users in the system, but secure communication is guaranteed only for one of the receivers. We show that mean based or artificial noise based transmission achieves the secrecy capacity of this model. Next, we impose *maximum* power constraints as opposed to *minimum* power constraints at the receivers. This corresponds to a cognitive radio setting where we control the received interference power at users. In this case, we show that ordinary Gaussian signalling is sufficient, and there is no need for mean or artificial noise signalling. Next, we drop the secrecy constraint and consider the classical MIMO broadcast channel (BC) with *minimum* receiver-side power constraints. This models an unsecured communication scenario where simultaneous power and information transfer is needed for both users. We prove that dirty paper coding (DPC) used in [11] is optimal to achieve the capacity. This result intuitively verifies that, even though we need *minimum* received power guarantees, neither mean or artificial noise transmission is needed, because the freedom afforded by the design of the covariance matrices of the DPC scheme suffices to achieve all desired feasible receiver-side powers. Finally, we put back the secrecy constraints for both users and consider the BC with confidential messages BCCM [20]. We show that secure DPC (S-DPC) is optimal for the BCCM as in [20] without the need for mean or artificial noise signalling.

II. SYSTEM MODEL, PRELIMINARIES AND THE MAIN RESULT

The MIMO wiretap channel with N_t antennas at the transmitter, N_r antennas at the legitimate receiver and N_e antennas at the eavesdropper is given by (see Fig. 1),

$$\mathbf{Y}_i = \mathbf{H}\mathbf{X}_i + \mathbf{W}_{1,i} \quad (1)$$

$$\mathbf{Z}_i = \mathbf{G}\mathbf{X}_i + \mathbf{W}_{2,i} \quad (2)$$

where $\mathbf{X}_i \in \mathbb{R}^{N_t}$ is the channel input, $\mathbf{Y}_i \in \mathbb{R}^{N_r}$ is the legitimate receiver's channel output, and $\mathbf{Z}_i \in \mathbb{R}^{N_e}$ is the eavesdropper's channel output at channel use i ; $\mathbf{W}_{1,i}$ and $\mathbf{W}_{2,i}$ are independent Gaussian random vectors $\mathcal{N}(\mathbf{0}, \mathbf{I})$. The channel matrices of legitimate receiver \mathbf{H} and

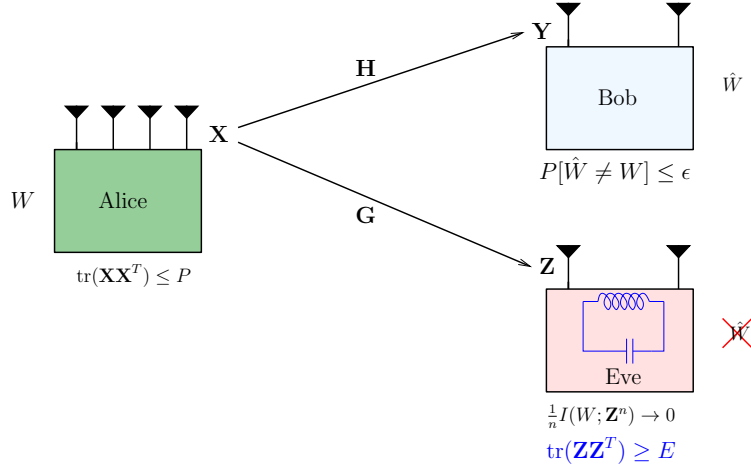


Fig. 1. Gaussian MIMO wiretap channel with receiver-side power constraint.

the eavesdropper \mathbf{G} are real-valued matrices of dimensions $N_r \times N_t$ and $N_e \times N_t$, respectively, and are fixed and known to all entities. The transmitter encodes a message W picked from a discrete message set \mathcal{W} to a codeword \mathbf{X}^n over n channel uses via a stochastic encoder $f : \mathcal{W} \rightarrow \mathbf{X}^n$. The channel input is constrained by the usual *maximum* average power constraint [25], [26]:

$$\frac{1}{n} \sum_{i=1}^n \text{tr}(\mathbf{X}_i \mathbf{X}_i^T) \leq P \quad (3)$$

In this paper, we consider *minimum* and *maximum* power constraints at the receivers. In the initial part of the paper, we consider a *minimum* power constraint at the eavesdropper only as:

$$\frac{1}{n} \sum_{i=1}^n \text{tr}(\mathbf{Z}_i \mathbf{Z}_i^T) \geq E \quad (4)$$

As usual, see [25], [26], the actual power constraints in (3) and (4) will be reflected in the single-letter capacity expressions in the sequel as expectations, i.e., $\text{tr}(\mathbb{E}[\mathbf{X}\mathbf{X}^T]) \leq P$ and $\text{tr}(\mathbb{E}[\mathbf{Z}\mathbf{Z}^T]) \geq E$. In addition, for all $\epsilon_n > 0$, we have the following asymptotic reliability and secrecy constraints on W based on n -length observations $\mathbf{Y}^n, \mathbf{Z}^n$ at the receiver and the eavesdropper, respectively:

$$\mathbb{P}[\hat{W} \neq W] \leq \epsilon_n, \quad \lim_{n \rightarrow \infty} \frac{1}{n} I(W; \mathbf{Z}^n) = 0 \quad (5)$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$, and $\hat{W} = \phi(\mathbf{Y}^n)$ is the estimate of the legitimate receiver of the transmitted message W based on \mathbf{Y}^n by using a decoder $\phi(\cdot)$.

In this case, we have an achievable rate $R_s(E, P, \mathbf{H}, \mathbf{G}) = \lim_{n \rightarrow \infty} \frac{1}{n} \log |\mathcal{W}|$ if there exists a code, i.e., a codebook and (f, ϕ) pair such that constraints (3)-(5) are satisfied. The secrecy capac-

ity $C(E, P, \mathbf{H}, \mathbf{G}) = \sup R(E, P, \mathbf{H}, \mathbf{G})$, i.e., the supremum of all achievable rates. Although, we will determine the secrecy capacity under the maximum transmitter-side power constraint in (3) and the minimum receiver-side power constraint in (4), we initially characterize $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$, the secrecy capacity, under a general *double-sided correlation matrix constraint*:

$$\mathbf{S}_1 \preceq \mathbf{Q} \preceq \mathbf{S}_2 \quad (6)$$

where $\mathbf{Q} = \mathbb{E}[\mathbf{X}\mathbf{X}^T]$ is the channel input correlation matrix, and $\mathbf{S}_1 \preceq \mathbf{S}_2$ are given and fixed positive semi-definite (PSD) matrices, where \preceq denotes the partial ordering of PSD matrices. We will show in a similar way to [11, Section II.B] that the secrecy capacity with power constraints of (3)-(4) can be obtained from the secrecy capacity with the more general double-sided correlation matrix constraint in (6) by maximizing this secrecy capacity over all correlation matrices $\mathbf{S}_1 \preceq \mathbf{S}_2$ that lie in the compact set \mathcal{S}_{PE} :

$$\mathcal{S}_{PE} = \{\mathbf{S} \succeq \mathbf{0} : \text{tr}(\mathbf{S}) \leq P, \quad \text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T) \geq \tilde{E}\} \quad (7)$$

where $\tilde{E} = E - N_e$. We evaluate the secrecy capacity based on Csiszar-Korner secrecy capacity expression [5]

$$C_s = \max_{V \rightarrow \mathbf{X} \rightarrow \mathbf{Y}, \mathbf{Z}} I(V; \mathbf{Y}) - I(V; \mathbf{Z}) \quad (8)$$

where V carries the message signal and \mathbf{X} is the channel input. The maximization is over all jointly distributed (V, \mathbf{X}) that satisfy the Markov chain $V \rightarrow \mathbf{X} \rightarrow \mathbf{Y}, \mathbf{Z}$ and the constraints (3), (4). Note that although Csiszar-Korner expression is initially given for discrete alphabets, it can be directly extended to alphabets other than discrete, by including the appropriate cost function in the maximization problem; see remarks in [5, Section VI]. This extension can be done via discrete approximations in [27, Chapter 3] and [28, Chapter 7].

The main result of this paper is the exact characterization of the secrecy capacity of the MIMO wiretap channel under the maximum transmitter-side power constraint in (3) and the minimum receiver-side power constraint in (4). This result is stated in Theorem 1 below. We dedicate Section III for the achievability proof and Section IV for the converse proof of this theorem. In Section V, we extend this basic proof technique to the cases of: minimum receiver-side power constraints at both receivers; maximum receiver-side power constraints; no secrecy constraints

(classical BC); and double-sided secrecy constraints (BCCM).

Theorem 1 *The secrecy capacity of a MIMO wiretap channel with a transmitter-side power constraint P and a receiver-side power constraint E , $C(E, P, \mathbf{H}, \mathbf{G})$, is given as*

$$C(E, P, \mathbf{H}, \mathbf{G}) = \max_{\mathbf{Q} \succeq \mathbf{0}, \boldsymbol{\mu}} \frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}\mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}\mathbf{G}^T|$$

$$\text{s.t. } \text{tr}(\mathbf{Q} + \boldsymbol{\mu}\boldsymbol{\mu}^T) \leq P, \quad \text{tr}(\mathbf{G}(\mathbf{Q} + \boldsymbol{\mu}\boldsymbol{\mu}^T)\mathbf{G}^T) \geq \tilde{E} \quad (9)$$

where $\tilde{E} = E - N_e$. This secrecy capacity is achieved by $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu}, \mathbf{Q})$, i.e., with a mean but no channel prefixing. Alternatively, the secrecy capacity, $C(E, P, \mathbf{H}, \mathbf{G})$, is also given as

$$C(E, P, \mathbf{H}, \mathbf{G}) = \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T|}{|\mathbf{I} + \mathbf{H}\mathbf{Q}_2\mathbf{H}^T|} - \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T|}{|\mathbf{I} + \mathbf{G}\mathbf{Q}_2\mathbf{G}^T|}$$

$$\text{s.t. } \text{tr}(\mathbf{Q}_1 + \mathbf{Q}_2) \leq P, \quad \text{tr}(\mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E} \quad (10)$$

where $\mathbf{X} = \mathbf{V} + \mathbf{U}$, with jointly Gaussian $\mathbf{V} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_1)$ and $\mathbf{U} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_2)$, and \mathbf{V}, \mathbf{U} are independent, i.e., with Gaussian signalling with Gaussian channel prefixing.

III. ACHIEVABILITY SCHEMES

In this section, we provide two coding schemes that achieve the secrecy capacity of the MIMO wiretap channel with transmitter and receiver-side power constraints given in Theorem 1.

A. Gaussian Coding with Fixed Mean

The first achievable scheme is Gaussian coding with fixed mean, i.e., $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu}, \mathbf{Q}_1)$. In this case, the fixed mean does not play a role in evaluating the secrecy capacity except for consuming part of the overall correlation matrix and only provides the required power level at the receiver side. Then, we choose $\mathbf{V} = \mathbf{X}$, i.e., no channel prefixing. Hence, we have

$$C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \geq \max_{\mathbf{Q}_1 \succeq \mathbf{0}, \boldsymbol{\mu}} I(\mathbf{X}; \mathbf{Y}) - I(\mathbf{X}; \mathbf{Z})$$

$$= \max_{\mathbf{Q}_1 \succeq \mathbf{0}, \boldsymbol{\mu}} \frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}_1\mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}_1\mathbf{G}^T|$$

$$\text{s.t. } \mathbf{S}_1 \preceq \mathbf{Q}_1 + \boldsymbol{\mu}\boldsymbol{\mu}^T \preceq \mathbf{S}_2 \quad (11)$$

In the converse proof, in place of $\boldsymbol{\mu}\boldsymbol{\mu}^T$, we have a general positive semidefinite matrix \mathbf{Q}_2 . In order to have a matching feasible coding scheme, \mathbf{Q}_2 must be constrained to unit-rank correlation

matrices, as it corresponds to the mean of the transmitted signal. Although, the solution of \mathbf{Q}_2 is generally not unit-rank for arbitrary correlation matrices $\mathbf{S}_1, \mathbf{S}_2$, we show in the following lemma that for the special case of a maximum transmitter-side power constraint P and a minimum receiver-side power constraint E , the solution is guaranteed to be of unit-rank, and hence the mean based coding scheme is feasible.

Lemma 1 *The coding scheme $\mathbf{X} \sim \mathcal{N}(\mathbb{V}(\mathbf{Q}_2^*), \mathbf{Q}_1^*)$ is achievable for the wiretap channel under the transmitter-side power constraint P and the receiver-side power constraint E given that the matrix $\mathbf{G}^T \mathbf{G}$ has a unique maximum eigenvalue. The secrecy rate is characterized by the following optimization problem:*

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \frac{1}{2} \log |\mathbf{I} + \mathbf{H} \mathbf{Q}_1 \mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G} \mathbf{Q}_1 \mathbf{G}^T| \\ \text{s.t.} \quad & \text{tr}(\mathbf{Q}_1 + \mathbf{Q}_2) \leq P, \quad \text{tr}(\mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E} \end{aligned} \quad (12)$$

where $\mathbf{Q}_1^*, \mathbf{Q}_2^*$ are the optimal correlation matrices for (12) and $\mathbb{V}(\mathbf{Q}_2^*)$ denotes the unique eigenvector of matrix \mathbf{Q}_2^* with a non-zero eigenvalue.

Proof: We note that \mathbf{Q}_2 does not appear in the objective function; it only appears in the constraint set. Therefore, its only role is to enlarge the feasible set for \mathbf{Q}_1 subject to some power constraint \tilde{P} , where $\tilde{P} \leq P$. Thus, \mathbf{Q}_2 must be chosen such that, when the first constraint of (12) is fixed, it maximizes the feasible set for \mathbf{Q}_1 in the second constraint, i.e., \mathbf{Q}_2 must be the solution of

$$\max_{\mathbf{Q}_2 \succeq \mathbf{0}} \quad \text{tr}(\mathbf{G} \mathbf{Q}_2 \mathbf{G}^T) \quad \text{s.t.} \quad \text{tr}(\mathbf{Q}_2) = \tilde{P} \quad (13)$$

The eigenvector decomposition for \mathbf{Q}_2 , which is symmetric, is

$$\mathbf{Q}_2 = \sum_{i=1}^r \lambda_i \mathbf{q}_i \mathbf{q}_i^T \quad (14)$$

where $r, \lambda_i, \mathbf{q}_i$ are the rank, the i th eigenvalue and the corresponding orthonormal eigenvector of \mathbf{Q}_2 , respectively. Thus, we can write the constraint as $\text{tr}(\mathbf{Q}_2) = \sum_{i=1}^r \lambda_i = \tilde{P}$. Moreover, the objective function can be written as

$$\text{tr}(\mathbf{G} \mathbf{Q}_2 \mathbf{G}^T) = \text{tr} \left(\mathbf{G} \left(\sum_{i=1}^r \lambda_i \mathbf{q}_i \mathbf{q}_i^T \right) \mathbf{G}^T \right) = \sum_{i=1}^r \lambda_i \|\mathbf{G} \mathbf{q}_i\|^2 \quad (15)$$

Hence, the optimization problem in (13) can be written as

$$\max_{\lambda_i, \mathbf{q}_i} \sum_{i=1}^r \lambda_i \|\mathbf{G}\mathbf{q}_i\|^2 \quad \text{s.t.} \quad \sum_{i=1}^r \lambda_i = \tilde{P} \quad (16)$$

which is a linear program in λ_i . The optimum solution is $\lambda_m = \tilde{P}$, and $\lambda_i = 0$ for $i \neq m$, where

$$m = \arg \max_i \|\mathbf{G}\mathbf{q}_i\|^2 \quad (17)$$

Hence, the optimal solution for this problem is to beam-form all the available power \tilde{P} to the direction of the largest $\|\mathbf{G}\mathbf{q}_i\|^2$. This solution is unique if $\mathbf{G}^T\mathbf{G}$ has a unique maximum eigenvalue. Otherwise a unit-rank solution for \mathbf{Q}_2 is not guaranteed. In this case, $\mathbf{Q}_2 = \tilde{P}\mathbf{q}_m\mathbf{q}_m^T$, i.e., it is unit-rank with eigenvector $\boldsymbol{\mu} = \sqrt{\tilde{P}}\mathbf{q}_m$, and the problem is feasible. ■

We remark that the same capacity expression in (12) can be realized by letting $\mathbf{X} = \mathbf{V} + \mathbf{U}$, where $\mathbf{V} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_1)$ is the message-carrying signal and $\mathbf{U} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_2)$ is the energy-carrying signal that is known causally at both Bob and Eve, so that it can be cancelled prior to information decoding. We note that, with this coding scheme any covariance matrix \mathbf{Q}_2 can be realized, and therefore Lemma 1 is not needed with this coding scheme, i.e., that the converse and achievability match for all $\mathbf{S}_1, \mathbf{S}_2$. However, if \mathbf{Q}_2 is optimized for this scheme as well for given P, E , then the optimum \mathbf{Q}_2 is still unit-rank. If the problem is considered under covariance constraints, as opposed to power constraints, unit-rank requirement of the mean based scheme can be removed by sending known Gaussian signals instead, at the cost of extra overhead of identifying \mathbf{U} causally at Bob and Eve.

B. Gaussian Coding with Gaussian Artificial Noise

The second achievable scheme is Gaussian coding with Gaussian artificial noise. In this case, we choose $\mathbf{X} = \mathbf{V} + \mathbf{U}$, where \mathbf{V}, \mathbf{U} are independent and $\mathbf{V} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_1)$ and $\mathbf{U} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_2)$. Here, \mathbf{V} carries the message, \mathbf{X} is the channel input, and \mathbf{U} is the artificial noise (or cooperative jamming [13]) signal. In this case, we use channel prefixing, hence $\mathbf{V} \neq \mathbf{X}$. The extra randomness \mathbf{U} is sent by the transmitter to provide extra noise floor at both receivers, and confuses the eavesdropper. The added significance of this artificial noise in our problem is to provide a suitable level of received power at the receiver, i.e., we utilize the artificial noise as a source of

power. In this case, the achievable secrecy rate satisfies

$$\begin{aligned}
C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) &\geq \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} I(\mathbf{V}; \mathbf{Y}) - I(\mathbf{V}; \mathbf{Z}) \\
&= \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T|}{|\mathbf{I} + \mathbf{H}\mathbf{Q}_2\mathbf{H}^T|} - \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T|}{|\mathbf{I} + \mathbf{G}\mathbf{Q}_2\mathbf{G}^T|} \\
&\quad \text{s.t. } \mathbf{S}_1 \preceq \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2
\end{aligned} \tag{18}$$

IV. CONVERSE PROOF

In this section, we prove the reverse implication using the channel enhancement technique [10], [11]. We will consider the case of $\mathbf{S}_2 \succeq \mathbf{S}_1 \succ \mathbf{0}$ and the aligned MIMO setting which means that the channel matrices are square and invertible. The general MIMO case follows directly from the limiting arguments in [10], as the additional receiver-side power constraint is irrelevant in the limit. The idea of this limiting argument is to perform singular-value decomposition of the perturbed channels $\bar{\mathbf{H}}, \bar{\mathbf{G}}$ [10, Eqn. (37)]. Our result follows by taking the limit of this perturbation to zero. The argument is introduced in [10, Section II.B] and used for example in [20, Appendix B.2], [29, Section VII]. Therefore, we focus on the aligned case here. The aligned MIMO model is obtained by multiplying the input-output relations (1)-(2) by the inverse of the channel matrices:

$$\tilde{\mathbf{Y}} = \mathbf{X} + \mathbf{H}^{-1}\mathbf{W}_1 = \mathbf{X} + \tilde{\mathbf{W}}_1 \tag{19}$$

$$\tilde{\mathbf{Z}} = \mathbf{X} + \mathbf{G}^{-1}\mathbf{W}_2 = \mathbf{X} + \tilde{\mathbf{W}}_2 \tag{20}$$

where $\tilde{\mathbf{W}}_1$ and $\tilde{\mathbf{W}}_2$ are the equivalent zero-mean Gaussian random vectors with covariance matrices $\mathbf{N}_1 = \mathbf{H}^{-1}\mathbf{H}^{-T}$ and $\mathbf{N}_2 = \mathbf{G}^{-1}\mathbf{G}^{-T}$, respectively.

A. Equivalence of a Double-Sided Correlation Matrix Constraint

For the MIMO broadcast and wiretap channels under a transmitter-side maximum power constraint, references [10], [11] showed that it is sufficient to prove the converse under a maximum correlation constraint on the channel input. We first note here that in our case with maximum transmitter-side and minimum receiver-side power constraints, a single correlation constraint on the channel input, i.e., $\mathbf{Q} \preceq \mathbf{S}$, is not sufficient. Next, we show the equivalence of solving our problem with a *double-sided* correlation matrix constraint on the channel input,

i.e., $\mathbf{S}_1 \preceq \mathbf{Q} \preceq \mathbf{S}_2$. Then, our problem can be solved in two stages: the inner problem finds the capacity under fixed correlation matrices \mathbf{S}_1 and \mathbf{S}_2 constraints, and the outer problem finds the optimal $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}$ in (7). Finally, we modify the original channel enhancement technique [10], [11] to prove the optimality of the achievable schemes presented in the previous section.

We first note that solving the problem for $\mathbf{Q} \preceq \mathbf{S}$, where $\mathbf{S} \in \mathcal{S}_{PE}$ is insufficient. Consider solving the secrecy capacity under maximum transmitter-side and minimum receiver-side power constraints in two stages, first, solving the problem under a fixed correlation matrix \mathbf{S} , and then choosing the optimal $\mathbf{S} \in \mathcal{S}_{PE}$, i.e.,

$$\max_{\mathbf{S} \in \mathcal{S}_{PE}} \max_{\mathbf{Q} \preceq \mathbf{S}} R_s(\mathbf{Q}, \mathbf{H}, \mathbf{G}) \quad (21)$$

where $R_s(\mathbf{Q}, \mathbf{H}, \mathbf{G})$ is the achievable secure rate upon using correlation matrix \mathbf{Q} . Since $\mathbf{Q} \preceq \mathbf{S}$, we have $\mathbf{G}\mathbf{Q}\mathbf{G}^T \preceq \mathbf{G}\mathbf{S}\mathbf{G}^T$ and hence $\text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^T) \leq \text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T)$. Then, although any $\mathbf{S} \in \mathcal{S}_{PE}$ satisfies the minimum receiver-side power constraint, i.e., $\text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T) \geq \tilde{E}$, the input correlation matrix \mathbf{Q} is not guaranteed to satisfy $\text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^T) \geq \tilde{E}$. Hence, the single correlation constraint is not sufficient for solving problems involving minimum receiver-side power constraints.

Lemma 2 *Since \mathcal{S}_{PE} is a compact set of PSD matrices, and $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ is continuous with respect to \mathbf{S}_2 , we have*

$$C(E, P, \mathbf{H}, \mathbf{G}) = \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}, \mathbf{S}_1 \preceq \mathbf{S}_2} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (22)$$

Proof: We follow and extend the proof technique in [11, Lemma 1] to the case of double-sided covariance matrices. We define the wiretap code $\mathcal{C}(n, \mathbf{S}, R, \epsilon)$ as a codebook, where the codewords $\{\mathbf{X}_i^n\}_{i=1}^{2^{nR}}$ are such that $\mathbf{S} = \frac{1}{2^{nR}} \sum_{i=1}^{2^{nR}} \mathbf{X}_i^n \mathbf{X}_i^{nT}$, and accompanying encoding and decoding functions (f, ϕ) , such that $\mathbb{P}(\phi(f(W)) \neq W) \leq \epsilon$. The decoder ϕ can be taken as the maximum likelihood decoder.

To see

$$C(E, P, \mathbf{H}, \mathbf{G}) \geq \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}, \mathbf{S}_1 \preceq \mathbf{S}_2} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (23)$$

we note that for any $\mathbf{S}_1 \preceq \mathbf{Q} \preceq \mathbf{S}_2$ where $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}$, we have $\mathbf{Q} \in \mathcal{S}_{PE}$, i.e., every \mathbf{Q} in the feasible set of the optimization problem on the right hand side belongs to the feasible

set of the optimization problem $C(E, P, \mathbf{H}, \mathbf{G})$. Hence, $C(E, P, \mathbf{H}, \mathbf{G})$ is at least as large as $\max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}, \mathbf{S}_1 \preceq \mathbf{S}_2} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$.

To see

$$C(E, P, \mathbf{H}, \mathbf{G}) \leq \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}, \mathbf{S}_1 \preceq \mathbf{S}_2} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (24)$$

we should prove that $C(E, P, \mathbf{H}, \mathbf{G}) = C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ for some $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}$ [11]. If $R = C(E, P, \mathbf{H}, \mathbf{G})$ is achievable, then there exists an infinite sequence of codes $\mathcal{C}(n_i, \mathbf{S}_{0_i}, R, \epsilon_i)$, $i = 1, \dots$ with rate R and decreasing probability of error $\epsilon_i \rightarrow 0$ as $i \rightarrow \infty$. Choose $\mathbf{S}_1 \preceq \mathbf{S}_{0_i}$, $\forall i$ and $\mathbf{S}_1 \in \mathcal{S}_{PE}$. We note that the choice of \mathbf{S}_1 is completely arbitrary, thus without loss of generality, we can choose it to be the first element in the sequence, i.e., \mathbf{S}_{0_1} . As \mathcal{S}_{PE} is compact [30], [31], for any infinite sequence of points in \mathcal{S}_{PE} , there must exist a sub-sequence that converges to a point $\mathbf{S}_0 \in \mathcal{S}_{PE}$. Hence, for any arbitrary $\delta > 0$, we can find an increasing subsequence $i(k)$ such that $\mathbf{S}_1 \preceq \mathbf{S}_{0_{i(k)}} \preceq \mathbf{S}_0 + \delta \mathbf{I}$.

This implies that we can find a sequence of codes $\mathcal{C}(n_k, \mathbf{S}_0 + \delta \mathbf{I}, R, \epsilon_k)$ with $\mathbf{S}_0 \in \mathcal{S}_{PE}$, $\mathbf{S}_0 \succeq \mathbf{S}_1$ achieving small probability of error. Therefore, for every $\delta > 0$, we have $R = C(\mathbf{S}_1, \mathbf{S}_0 + \delta \mathbf{I}, \mathbf{H}, \mathbf{G})$. Since $C(\mathbf{S}_1, \mathbf{S}_0 + \delta \mathbf{I}, \mathbf{H}, \mathbf{G})$ is continuous, see Appendix A, with respect to its second argument, we have that every ϵ -ball around R contains $C(\mathbf{S}_1, \mathbf{S}_0, \mathbf{H}, \mathbf{G})$, since for every $\epsilon > 0$, there exists $\delta > 0$ such that $C(\mathbf{S}_1, \mathbf{S}_0 + \delta \mathbf{I}, \mathbf{H}, \mathbf{G}) - C(\mathbf{S}_1, \mathbf{S}_0, \mathbf{H}, \mathbf{G}) < \epsilon$ as continuity asserts. Therefore R is a limit point of $C(\mathbf{S}_1, \mathbf{S}_0, \mathbf{H}, \mathbf{G})$ and hence $C(E, P, \mathbf{H}, \mathbf{G}) = C(\mathbf{S}_1, \mathbf{S}_0, \mathbf{H}, \mathbf{G})$. This limit point belongs to \mathcal{S}_{PE} since it is closed. ■

B. Converse Proof for Gaussian Coding with Fixed Mean

First, we begin with writing the equivalent optimization problem corresponding to the achievability scheme in the aligned MIMO case with Gaussian coding $\mathbf{X} \sim \mathcal{N}(\mathbb{V}(\mathbf{Q}_2^*), \mathbf{Q}_1^*)$:

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{N}_1|}{|\mathbf{N}_1|} - \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{N}_2|}{|\mathbf{N}_2|} \\ \text{s.t.} \quad & \mathbf{Q}_1 + \mathbf{Q}_2 \succeq \mathbf{S}_1, \quad \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2 \end{aligned} \quad (25)$$

The Lagrangian of this optimization problem can be written as:

$$\mathcal{L} = \log \frac{|\mathbf{Q}_1 + \mathbf{N}_2|}{|\mathbf{N}_2|} - \log \frac{|\mathbf{Q}_1 + \mathbf{N}_1|}{|\mathbf{N}_1|} - \text{tr}(\mathbf{Q}_1 \mathbf{M}_1) - \text{tr}(\mathbf{Q}_2 \mathbf{M}_2) - \text{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_1) \mathbf{M}_3)$$

$$+ \text{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_2)\mathbf{M}_4) \quad (26)$$

where $\mathbf{M}_1 \succeq \mathbf{0}$, $\mathbf{M}_2 \succeq \mathbf{0}$, $\mathbf{M}_3 \succeq \mathbf{0}$ and $\mathbf{M}_4 \succeq \mathbf{0}$ are the Lagrange multipliers for each constraint.

The corresponding KKT complementary slackness conditions are:

$$\mathbf{Q}_1^* \mathbf{M}_1 = \mathbf{0}, \quad \mathbf{Q}_2^* \mathbf{M}_2 = \mathbf{0} \quad (27)$$

$$(\mathbf{Q}_1^* + \mathbf{Q}_2^* - \mathbf{S}_1)\mathbf{M}_3 = \mathbf{0} \quad (28)$$

$$(\mathbf{S}_2 - \mathbf{Q}_1^* - \mathbf{Q}_2^*)\mathbf{M}_4 = \mathbf{0} \quad (29)$$

and the KKT optimality conditions for \mathbf{Q}_1^* and \mathbf{Q}_2^* are:

$$(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} - \mathbf{M}_1 - \mathbf{M}_3 + \mathbf{M}_4 = \mathbf{0} \quad (30)$$

$$-\mathbf{M}_2 - \mathbf{M}_3 + \mathbf{M}_4 = \mathbf{0} \quad (31)$$

Now, using (30) and (31), we can construct an enhanced channel that can serve as an upper bound for the original legitimate receiver's channel, while the eavesdropper's channel is degraded with respect to it. The covariance of the enhanced channel is chosen as $\tilde{\mathbf{N}}$ such that

$$(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 = (\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 = (\mathbf{Q}_1^* + \tilde{\mathbf{N}})^{-1} \quad (32)$$

Using this definition of the enhanced channel, we explore various characteristics of $\tilde{\mathbf{N}}$.

First, to prove the validity of the covariance matrix $\tilde{\mathbf{N}}$, we note that

$$\tilde{\mathbf{N}} = [(\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1]^{-1} - \mathbf{Q}_1^* \quad (33)$$

$$= (\mathbf{I} + \mathbf{N}_1 \mathbf{M}_1)^{-1} (\mathbf{Q}_1^* + \mathbf{N}_1) - \mathbf{Q}_1^* \quad (34)$$

$$= (\mathbf{I} + \mathbf{N}_1 \mathbf{M}_1)^{-1} [(\mathbf{Q}_1^* + \mathbf{N}_1) - (\mathbf{I} + \mathbf{N}_1 \mathbf{M}_1) \mathbf{Q}_1^*] \quad (35)$$

$$= (\mathbf{I} + \mathbf{N}_1 \mathbf{M}_1)^{-1} \mathbf{N}_1 = (\mathbf{N}_1^{-1} + \mathbf{M}_1)^{-1} \succeq \mathbf{0} \quad (36)$$

and hence the covariance matrix of the constructed enhanced channel is positive semi-definite, and therefore it is a feasible covariance matrix.

Next, we want to show that the constructed channel is enhanced with respect to \mathbf{N}_1 , i.e., $\mathbf{N}_1 \succeq \tilde{\mathbf{N}}$. To show that we note from (36) that $\tilde{\mathbf{N}} = (\mathbf{N}_1^{-1} + \mathbf{M}_1)^{-1}$ and hence, $\mathbf{N}_1 \succeq \tilde{\mathbf{N}}$. Similarly by considering $(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 = (\mathbf{Q}_1^* + \tilde{\mathbf{N}})^{-1}$ we note that $\mathbf{N}_2 \succeq \tilde{\mathbf{N}}$. Hence, we conclude that

the enhanced channel has better channel conditions than the original legitimate user's channel, therefore, the constructed channel is an upper bound for the legitimate receiver. Moreover, the eavesdropper's channel is degraded with respect to the constructed channel. Consequently the secrecy capacity of the enhanced channel is known. In other words, we have $\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{W}}$ such that $\tilde{\mathbf{W}} \sim \mathcal{N}(\mathbf{0}, \tilde{\mathbf{N}})$ and $\mathbf{X} \rightarrow \tilde{\mathbf{Y}} \rightarrow \mathbf{Y}$ and $\mathbf{X} \rightarrow \tilde{\mathbf{Y}} \rightarrow \mathbf{Z}$.

In order to have a meaningful upper bound, we need to show that the rate is preserved between the original problem and the constructed channel. To show that, we have

$$(\mathbf{Q}_1^* + \tilde{\mathbf{N}})^{-1} \tilde{\mathbf{N}} = (\mathbf{Q}_1^* + \tilde{\mathbf{N}})^{-1} (\tilde{\mathbf{N}} + \mathbf{Q}_1^* - \mathbf{Q}_1^*) \quad (37)$$

$$= \mathbf{I} - (\mathbf{Q}_1^* + \tilde{\mathbf{N}})^{-1} \mathbf{Q}_1^* \quad (38)$$

$$= \mathbf{I} - [(\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1] \mathbf{Q}_1^* \quad (39)$$

$$= \mathbf{I} - (\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} \mathbf{Q}_1^* = (\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} \mathbf{N}_1 \quad (40)$$

where (39) follows from the definition of the enhanced channel and (40) follows from the complementary slackness condition (27). Therefore, we have

$$\frac{|\tilde{\mathbf{N}} + \mathbf{Q}_1^*|}{|\tilde{\mathbf{N}}|} = \frac{|\mathbf{N}_1 + \mathbf{Q}_1^*|}{|\mathbf{N}_1|} \quad (41)$$

To show a similar rate preservation argument for the degraded channel \mathbf{N}_2 , we will need the following lemma.

Lemma 3 *The optimal covariance matrix for the achievable scheme with Gaussian signaling with a fixed mean \mathbf{Q}_1^* satisfies $(\mathbf{S}_2 - \mathbf{Q}_1^*)\mathbf{M}_2 = \mathbf{0}$.*

Proof: We return to the KKT conditions. Considering the correlation constraint, three cases can possibly occur. The first case: the correlation constraint is satisfied with equality, consequently $\mathbf{S}_2 - \mathbf{Q}_1^* = \mathbf{Q}_2^*$. In this case, $(\mathbf{S}_2 - \mathbf{Q}_1^*)\mathbf{M}_2 = \mathbf{Q}_2^*\mathbf{M}_2 = \mathbf{0}$ from (27). The second case: the correlation constraint is strictly loose, i.e., $\mathbf{Q}_1 + \mathbf{Q}_2 \prec \mathbf{S}_2$. In this case, we can define a matrix $\Delta = \mathbf{S}_2 - \mathbf{Q}_1^* - \mathbf{Q}_2^* \succ \mathbf{0}$, and therefore Δ is a full-rank matrix. Thus, $\mathbf{M}_4 = \mathbf{0}$ and from (31), we have $\mathbf{M}_2 = -\mathbf{M}_3$. The matrices $\mathbf{M}_2, \mathbf{M}_3$ are both positive semi-definite matrices. Therefore, we must have $\mathbf{M}_2 = \mathbf{M}_3 = \mathbf{0}$. Finally, the third case: the correlation constraint is partially loose, that is, we have $\Delta = \mathbf{S}_2 - \mathbf{Q}_1 - \mathbf{Q}_2 \succeq \mathbf{0}$, hence Δ is not a full-rank matrix. We define

$\Sigma = S_2 - S_1 \succ 0$, i.e., $S_1 = S_2 - \Sigma$. In this case, we sum the KKT conditions (28) and (29) to obtain the following implications:

$$(Q_1^* + Q_2^*)(M_3 - M_4) - S_1 M_3 + S_2 M_4 = 0 \quad (42)$$

$$(Q_1^* + Q_2^*)(M_3 - M_4) - S_2 M_3 + \Sigma M_3 + S_2 M_4 = 0 \quad (43)$$

$$(S_2 - Q_1^* - Q_2^*)(M_4 - M_3) = -\Sigma M_3 \quad (44)$$

$$(S_2 - Q_1^* - Q_2^*)M_2 = -\Sigma M_3 \quad (45)$$

$$(S_2 - Q_1^*)M_2 = -\Sigma M_3 \quad (46)$$

where (45) follows from (31), and (46) follows from (27). Since $(S_2 - Q_1^*)M_2 \succeq 0$ and $\Sigma M_3 \succeq 0$, or at least $(S_2 - Q_1^*)M_2$ and ΣM_3 have the same number of non-negative eigenvalues of M_2 and M_3 , respectively [32], the only way to satisfy (46) is to have all the eigenvalues of both matrices equal zero, i.e., $(S_2 - Q_1^*)M_2 = -\Sigma M_3 = 0$. Hence, we conclude that for all three cases we have $(S_2 - Q_1^*)M_2 = 0$ and this completes the proof of Lemma 3. ■

Hence, using Lemma 3, we write:

$$(\tilde{N} + S_2)(Q_1^* + \tilde{N})^{-1} = (S_2 - Q_1^*)(Q_1^* + \tilde{N})^{-1} + I \quad (47)$$

$$= (S_2 - Q_1^*)[(Q_1^* + N_2)^{-1} + M_2] + I \quad (48)$$

$$= (S_2 - Q_1^*)(Q_1^* + N_2)^{-1} + I \quad (49)$$

$$= [(N_2 + S_2) - (Q_1^* + N_2)](Q_1^* + N_2)^{-1} + I \quad (50)$$

$$= (N_2 + S_2)(Q_1^* + N_2)^{-1} \quad (51)$$

where (48) follows from the definition of the enhanced channel (32), and (49) follows from Lemma 3. Hence, we have:

$$\frac{|S_2 + \tilde{N}|}{|S_2 + N_2|} = \frac{|Q_1^* + \tilde{N}|}{|Q_1^* + N_2|} \quad (52)$$

We upper bound the secrecy capacity of the MIMO wiretap channel with a receiver-side power constraint by the secrecy capacity of the enhanced channel. Since $S_2 \in \mathcal{S}_{PE}$, S_2 satisfies the receiver power constraint for the enhanced channel. Hence, the receiver constraint is valid with

the upper bounding argument. The secrecy capacity of the enhanced channel \tilde{C}_s is given by

$$\tilde{C}_s = \frac{1}{2} \log \frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\tilde{\mathbf{N}}|} - \frac{1}{2} \log \frac{|\mathbf{S}_2 + \mathbf{N}_2|}{|\mathbf{N}_2|} \quad (53)$$

$$= \frac{1}{2} \log \frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{S}_2 + \mathbf{N}_2|} \cdot \frac{|\mathbf{N}_2|}{|\tilde{\mathbf{N}}|} \quad (54)$$

$$= \frac{1}{2} \log \frac{|\mathbf{Q}_1^* + \tilde{\mathbf{N}}|}{|\mathbf{Q}_1^* + \mathbf{N}_2|} \cdot \frac{|\mathbf{N}_2|}{|\tilde{\mathbf{N}}|} \quad (55)$$

$$= \frac{1}{2} \log \frac{|\mathbf{Q}_1^* + \tilde{\mathbf{N}}|}{|\tilde{\mathbf{N}}|} - \frac{1}{2} \log \frac{|\mathbf{Q}_1^* + \mathbf{N}_2|}{|\mathbf{N}_2|} \quad (56)$$

$$= \frac{1}{2} \log \frac{|\mathbf{Q}_1^* + \mathbf{N}_1|}{|\mathbf{N}_1|} - \frac{1}{2} \log \frac{|\mathbf{Q}_1^* + \mathbf{N}_2|}{|\mathbf{N}_2|} = C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (57)$$

where (55) follows from (52), and (57) follows from (41), completing the converse proof for the case of Gaussian signalling with a fixed mean.

C. Converse Proof for Gaussian Coding with Gaussian Artificial Noise

In this section, we follow a similar channel enhancement technique as in Section IV-B. The optimization problem corresponding to the Gaussian coding scheme with artificial noise is:

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2 + \mathbf{N}_1|} - \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_2|}{|\mathbf{Q}_2 + \mathbf{N}_2|} \\ \text{s.t.} \quad & \mathbf{Q}_1 + \mathbf{Q}_2 \succeq \mathbf{S}_1, \quad \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2 \end{aligned} \quad (58)$$

The Lagrangian for this optimization problem is given by:

$$\begin{aligned} \mathcal{L} = & \log \frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_2|}{|\mathbf{Q}_2 + \mathbf{N}_2|} - \log \frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2 + \mathbf{N}_1|} - \text{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_1)\mathbf{M}_3) \\ & - \text{tr}(\mathbf{Q}_1\mathbf{M}_1) - \text{tr}(\mathbf{Q}_2\mathbf{M}_2) + \text{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_2)\mathbf{M}_4) \end{aligned} \quad (59)$$

The complementary slackness conditions (27)-(29) are still the same due to the same set of constraints for both problems (58) and (25). The KKT optimality condition for \mathbf{Q}_1^* and \mathbf{Q}_2^* are:

$$(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \mathbf{M}_1 - \mathbf{M}_3 + \mathbf{M}_4 = \mathbf{0} \quad (60)$$

$$(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + (\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \mathbf{M}_2 - \mathbf{M}_3 + \mathbf{M}_4 = \mathbf{0} \quad (61)$$

Using (60), we can write (61) as:

$$\mathbf{M}_1 - (\mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + (\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \mathbf{M}_2 = \mathbf{0} \quad (62)$$

In this case, we again construct an enhanced channel with similar steps as in Section IV-B. The enhanced channel is constructed as:

$$(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 = (\mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 = (\mathbf{Q}_2^* + \tilde{\mathbf{N}})^{-1} \quad (63)$$

which is the same as in the previous section. Therefore, it follows that $\tilde{\mathbf{N}} \succeq \mathbf{0}$, $\tilde{\mathbf{N}} \preceq \mathbf{N}_1$, $\tilde{\mathbf{N}} \preceq \mathbf{N}_2$. Similarly, we can prove that the rate is preserved for the eavesdropper (as in the set of equations (37)-(41) with \mathbf{Q}_2^* instead of \mathbf{Q}_1^*), i.e.,

$$\frac{|\tilde{\mathbf{N}} + \mathbf{Q}_2^*|}{|\tilde{\mathbf{N}}|} = \frac{|\mathbf{N}_2 + \mathbf{Q}_2^*|}{|\mathbf{N}_2|} \quad (64)$$

To prove the rate preservation for the legitimate receiver, we will need the following lemma.

Lemma 4 *To achieve a positive secrecy rate using Gaussian coding with artificial noise, \mathbf{S}_2 must be fully used, i.e., $\mathbf{S}_2 = \mathbf{Q}_1^* + \mathbf{Q}_2^*$, and the optimal covariance matrix used for the artificial noise component, \mathbf{Q}_2^* , satisfies $(\mathbf{S}_2 - \mathbf{Q}_2^*)\mathbf{M}_1 = \mathbf{0}$.*

Proof: We start by proving the first part of the lemma by contradiction. Assume that a positive secrecy rate can be achieved using artificial noise, and \mathbf{S}_2 is partially used. Then, we have two cases. The first case: $\Delta = \mathbf{S}_2 - \mathbf{Q}_1^* - \mathbf{Q}_2^* \succ \mathbf{0}$. Hence, Δ is a full-rank matrix, then $\mathbf{M}_4 = \mathbf{0}$. From (60), we can write $(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 + \mathbf{M}_3 = (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1}$ and hence, $(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} \preceq (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1}$, which results in $\mathbf{N}_2 \preceq \mathbf{N}_1$. This means that the legitimate channel is degraded with respect to the eavesdropper channel, and hence, no positive secrecy rate can be achieved. This contradicts our assumption. The second case: Δ is not full-rank. Due to the similarity of the complementary slackness conditions for the artificial noise and the Gaussian coding with fixed mean settings, we have also (44), and from (60), we have

$$\mathbf{M}_4 - \mathbf{M}_3 = (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + \mathbf{M}_1 \quad (65)$$

substituting this in (44), we have the following implications:

$$\Delta(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \Delta(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + \Delta\mathbf{M}_1 = -\Sigma\mathbf{M}_3 \quad (66)$$

$$\Delta[(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - \Delta(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1}] = \Delta\mathbf{M}_1 + \Sigma\mathbf{M}_3 \quad (67)$$

Then, $[(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1}]^{-1} \succeq \mathbf{0}$ to have (67) hold true [33], and then we have $\mathbf{N}_2 \preceq \mathbf{N}_1$ as in the previous case, which also contradicts the assumption of having a positive secrecy rate. Hence, $\mathbf{Q}_1^* + \mathbf{Q}_2^* = \mathbf{S}_2$. For the second part of the lemma, we now have $\mathbf{S}_2 - \mathbf{Q}_2^* = \mathbf{Q}_1^*$, and from the complementary slackness condition $\mathbf{Q}_1^*\mathbf{M}_1 = \mathbf{0}$. Then, we conclude that $(\mathbf{S}_2 - \mathbf{Q}_2^*)\mathbf{M}_1 = \mathbf{0}$, completing the proof of Lemma 4. ■

Using Lemma 4, we can prove rate preservation for the legitimate receiver as follows:

$$(\tilde{\mathbf{N}} + \mathbf{S}_2)(\mathbf{Q}_2^* + \tilde{\mathbf{N}})^{-1} = (\mathbf{S}_2 - \mathbf{Q}_2^*)(\mathbf{Q}_2^* + \tilde{\mathbf{N}})^{-1} + \mathbf{I} \quad (68)$$

$$= (\mathbf{S}_2 - \mathbf{Q}_2^*)[(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1] + \mathbf{I} \quad (69)$$

$$= (\mathbf{S}_2 - \mathbf{Q}_2^*)(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{I} \quad (70)$$

$$= [(\mathbf{N}_1 + \mathbf{S}_2) - (\mathbf{Q}_2^* + \mathbf{N}_1)](\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{I} \quad (71)$$

$$= (\mathbf{N}_1 + \mathbf{S}_2)(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} \quad (72)$$

where (69) follows from the definition of the enhanced channel (63), and (70) follows from Lemma 4. Therefore, we have:

$$\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{Q}_2^* + \tilde{\mathbf{N}}|} = \frac{|\mathbf{S}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|} \quad (73)$$

Hence, the secrecy capacity of the enhanced channel is given by:

$$\tilde{C}_s = \frac{1}{2} \log \frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\tilde{\mathbf{N}}|} - \frac{1}{2} \log \frac{|\mathbf{S}_2 + \mathbf{N}_2|}{|\mathbf{N}_2|} \quad (74)$$

$$= \frac{1}{2} \log \frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{S}_2 + \mathbf{N}_2|} \cdot \frac{|\mathbf{N}_2|}{|\tilde{\mathbf{N}}|} \quad (75)$$

$$= \frac{1}{2} \log \frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{S}_2 + \mathbf{N}_2|} \cdot \frac{|\mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{Q}_2^* + \tilde{\mathbf{N}}|} \quad (76)$$

$$= \frac{1}{2} \log \frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{Q}_2^* + \tilde{\mathbf{N}}|} \cdot \frac{|\mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{S}_2 + \mathbf{N}_2|} \quad (77)$$

$$= \frac{1}{2} \log \frac{|\mathbf{S}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|} \cdot \frac{|\mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{S}_2 + \mathbf{N}_2|} \quad (78)$$

$$= \frac{1}{2} \log \frac{|\mathbf{S}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|} - \frac{1}{2} \log \frac{|\mathbf{S}_2 + \mathbf{N}_2|}{|\mathbf{Q}_2^* + \mathbf{N}_2|} \quad (79)$$

$$= \frac{1}{2} \log \frac{|\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|} - \frac{1}{2} \log \frac{|\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{Q}_2^* + \mathbf{N}_2|} = C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (80)$$

where (76) follows from (64), (78) follows from (73), and (80) follows from $\mathbf{Q}_1^* + \mathbf{Q}_2^* = \mathbf{S}_2$, completing the converse proof for the case of Gaussian signalling with Gaussian artificial noise.

V. EXTENSIONS TO RELATED CHANNEL MODELS

A. Gaussian MIMO Wiretap Channel Under Dual Minimum Receiver-Side Power Constraints

In this section, we consider the case where we impose dual receiver-side *minimum* power constraints, i.e., receiver-side power constraints both on the legitimate receiver and the eavesdropper. Then, we have the following constraint in addition to the constraints in (3) and (4):

$$\text{tr}(\mathbb{E}[\mathbf{Y}\mathbf{Y}^T]) \geq E_2 \quad (81)$$

where E_2 is the minimum power level that should be delivered to the legitimate receiver. The following theorem characterizes the secrecy capacity of this model.

Theorem 2 *The secrecy capacity of a MIMO wiretap channel with a transmitter-side power constraint P and dual receiver-side power constraints E_1, E_2 , $C(E_1, E_2, P, \mathbf{H}, \mathbf{G})$, is given as*

$$\begin{aligned} C(E_1, E_2, P, \mathbf{H}, \mathbf{G}) &= \max_{\mathbf{Q} \succeq \mathbf{0}, \boldsymbol{\mu}} \frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}\mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}\mathbf{G}^T| \\ \text{s.t.} \quad &\text{tr}(\mathbf{Q} + \boldsymbol{\mu}\boldsymbol{\mu}^T) \leq P \\ &\text{tr}(\mathbf{G}(\mathbf{Q} + \boldsymbol{\mu}\boldsymbol{\mu}^T)\mathbf{G}^T) \geq \tilde{E}_1, \quad \text{tr}(\mathbf{H}(\mathbf{Q} + \boldsymbol{\mu}\boldsymbol{\mu}^T)\mathbf{H}^T) \geq \tilde{E}_2 \end{aligned} \quad (82)$$

where $\tilde{E}_1 = E_1 - N_e$, and $\tilde{E}_2 = E - N_r$. This secrecy capacity is achieved by $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu}, \mathbf{Q})$, i.e., with a mean but no channel prefixing. Alternatively, $C(E_1, E_2, P, \mathbf{H}, \mathbf{G})$ is also given as

$$\begin{aligned} C(E_1, E_2, P, \mathbf{H}, \mathbf{G}) &= \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T|}{|\mathbf{I} + \mathbf{H}\mathbf{Q}_2\mathbf{H}^T|} - \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T|}{|\mathbf{I} + \mathbf{G}\mathbf{Q}_2\mathbf{G}^T|} \\ \text{s.t.} \quad &\text{tr}(\mathbf{Q}_1 + \mathbf{Q}_2) \leq P \\ &\text{tr}(\mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E}_1, \quad \text{tr}(\mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T) \geq \tilde{E}_2 \end{aligned} \quad (83)$$

where $\mathbf{X} = \mathbf{V} + \mathbf{U}$, with jointly Gaussian $\mathbf{V} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_1)$ and $\mathbf{U} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_2)$, where \mathbf{U}, \mathbf{V} are independent, i.e., Gaussian signalling with Gaussian channel prefixing.

Proof: The proof relies on verifying that the *double-sided correlation matrix constraint* constructed in Section IV-A is sufficient for this case also. First, we define the set $\mathcal{S}_{PE_1E_2}$ as:

$$\mathcal{S}_{PE_1E_2} = \{\mathbf{S} \succeq \mathbf{0} : \text{tr}(\mathbf{S}) \leq P, \quad \text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T) \geq \tilde{E}_1, \quad \text{tr}(\mathbf{H}\mathbf{S}\mathbf{H}^T) \geq \tilde{E}_2\} \quad (84)$$

To show the direct implication

$$C(E_1, E_2, P, \mathbf{H}, \mathbf{G}) \geq \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE_1E_2}, \mathbf{S}_1 \preceq \mathbf{S}_2} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (85)$$

we note that for any \mathbf{Q} such that $\mathbf{S}_1 \preceq \mathbf{Q} \preceq \mathbf{S}_2$ where $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE_1E_2}$, we have $\text{tr}(\mathbf{Q}) \leq \text{tr}(\mathbf{S}_2) \leq P$, $\text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^T) \geq \text{tr}(\mathbf{G}\mathbf{S}_1\mathbf{G}^T) \geq E_1$ and $\text{tr}(\mathbf{H}\mathbf{Q}\mathbf{H}^T) \geq \text{tr}(\mathbf{H}\mathbf{S}_1\mathbf{H}^T) \geq E_2$. Consequently, $\mathbf{Q} \in \mathcal{S}_{PE_1E_2}$, i.e., the feasible set under $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE_1E_2}$ is a subset of the feasible set under P, E_1, E_2 constraints. Moreover, $\mathcal{S}_{PE_1E_2} \subseteq \mathcal{S}_{PE}$ defined in Section II, and hence $\mathcal{S}_{PE_1E_2}$ is also a compact set. Hence the implication

$$C(E_1, E_2, P, \mathbf{H}, \mathbf{G}) \leq \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE_1E_2}, \mathbf{S}_1 \preceq \mathbf{S}_2} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (86)$$

can be proved by following the reverse implication (23) of the proof of Lemma 2 for the compact set $\mathcal{S}_{PE_1E_2}$, we can show that:

$$C(E_1, E_2, P, \mathbf{H}, \mathbf{G}) = \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE_1E_2}, \mathbf{S}_1 \preceq \mathbf{S}_2} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \quad (87)$$

Then, the inner problem under the dual receiver-side power constraints is identical to its counterpart under a single receiver-side power constraint on the eavesdropper side only. Consequently, achievability schemes of mean based and artificial noise based signalling are optimal for the dual receiver-side minimum power constraints.

It only remains to show that the achievable rates with Gaussian signalling with fixed mean match the converse, i.e., that when the covariance matrix representing the mean is left unrestricted for converse purposes, at the optimal, it takes a unit-rank so that it can be implemented with a mean vector in the achievability. That is, we need to show that Lemma 1 extends to the current setting under P, E_1, E_2 constraints. To show this, as a generalization of (13), we need to solve:

$$\max_{\mathbf{Q}_2 \succeq \mathbf{0}} \alpha_1 \text{tr}(\mathbf{G}\mathbf{Q}_2\mathbf{G}^T) + \alpha_2 \text{tr}(\mathbf{H}\mathbf{Q}_2\mathbf{H}^T) \quad \text{s.t.} \quad \text{tr}(\mathbf{Q}_2) = \tilde{P} \quad (88)$$

This optimization problem is equivalent to:

$$\max_{\lambda_i, \mathbf{q}_i} \sum_{i=1}^r \lambda_i (\alpha_1 \|\mathbf{G}\mathbf{q}_i\|^2 + \alpha_2 \|\mathbf{H}\mathbf{q}_i\|^2) \quad \text{s.t.} \quad \sum_{i=1}^r \lambda_i = \tilde{P} \quad (89)$$

which has a beam-forming optimal solution of assigning all \tilde{P} to \mathbf{q}_m such that

$$m = \arg \max_i \alpha_1 \|\mathbf{G}\mathbf{q}_i\|^2 + \alpha_2 \|\mathbf{H}\mathbf{q}_i\|^2 \quad (90)$$

and hence the optimal \mathbf{Q}_2 is unit-rank and the mean-based signalling is feasible. ■

B. Gaussian MIMO Wiretap Channel Under Maximum Receiver-Side Power Constraints

In this section, we consider the MIMO wiretap channel under *maximum* receiver-side power constraints. This generalizes Gastpar's problem [1] to include a secrecy requirement. In this case, we limit the interference at both receivers instead of maintaining the received power levels at both receivers as in Section II. Then, we impose the following constraints together with (3):

$$\text{tr}(\mathbb{E}[\mathbf{Z}\mathbf{Z}^T]) \leq E_1, \quad \text{tr}(\mathbb{E}[\mathbf{Y}\mathbf{Y}^T]) \leq E_2 \quad (91)$$

Theorem 3 *The secrecy capacity of the MIMO wiretap channel with a transmitter-side power constraint P and maximum receiver-side power constraints E_1, E_2 , $C(E_1, E_2, P, \mathbf{H}, \mathbf{G})$, is*

$$\begin{aligned} C(E_1, E_2, P, \mathbf{H}, \mathbf{G}) = \max_{\mathbf{Q} \succeq \mathbf{0}} \quad & \frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}\mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}\mathbf{G}^T| \\ \text{s.t.} \quad & \text{tr}(\mathbf{Q}) \leq P, \quad \text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^T) \leq \tilde{E}_1, \quad \text{tr}(\mathbf{H}\mathbf{Q}\mathbf{H}^T) \leq \tilde{E}_2 \end{aligned} \quad (92)$$

This secrecy capacity is achieved by $\mathbf{X} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q})$, i.e., neither mean or channel prefixing is required.

Proof: Similar to the previous section, we construct a suitable correlation matrix set $\mathcal{S}'_{PE_1E_2}$ as:

$$\mathcal{S}'_{PE_1E_2} = \{\mathbf{S} \succeq \mathbf{0} : \text{tr}(\mathbf{S}) \leq P, \quad \text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T) \leq \tilde{E}_1, \quad \text{tr}(\mathbf{H}\mathbf{S}\mathbf{H}^T) \leq \tilde{E}_2\} \quad (93)$$

Now, we show that, using a *single-sided* correlation matrix constraint $\mathbf{Q} \preceq \mathbf{S}$ is sufficient for *maximum* receiver-side power constraints, unlike the *double-sided* correlation constraint that was necessary for *minimum* receiver-side power constraints so far. Since, for all $\mathbf{Q} \preceq \mathbf{S}$, we have $\text{tr}(\mathbf{Q}) \leq \text{tr}(\mathbf{S}) \leq P$, $\text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^T) \leq \text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T) \leq \tilde{E}_1$ and $\text{tr}(\mathbf{H}\mathbf{Q}\mathbf{H}^T) \leq \text{tr}(\mathbf{H}\mathbf{S}\mathbf{H}^T) \leq \tilde{E}_2$, we

thus have $\mathbf{Q} \in \mathcal{S}'_{PE_1E_2}$. Moreover, the set $\mathcal{S}'_{PE_1E_2}$ is closed and bounded and hence compact. Consequently, we can find a sequence of codes $\mathcal{C}(n_k, \mathbf{S}_0 + \delta \mathbf{I}, R, \epsilon_k)$ with $\mathbf{S}_0 \in \mathcal{S}'_{PE_1E_2}$, achieving small probability of error, that has a limit point of $C(\mathbf{S}_0, \mathbf{H}, \mathbf{G})$ and hence

$$C(E_1, E_2, P, \mathbf{H}, \mathbf{G}) = \max_{\mathbf{S} \in \mathcal{S}'_{PE_1E_2}} C(\mathbf{S}, \mathbf{H}, \mathbf{G}) \quad (94)$$

Consequently, the inner problem under a correlation matrix constraint for the wiretap channel with maximum receiver-side power limitations is identical to the inner problem for the classical wiretap channel without the extra maximum receiver-side power constraints. Hence, the classical Gaussian coding with zero-mean and no channel-prefixing is optimal. ■

C. Gaussian MIMO Broadcast Channel Under Minimum Receiver-Side Power Constraints

In this section, we consider the MIMO BC with no secrecy constraints under *minimum* receiver-side power constraints. In this setting, the transmitter is required to communicate messages simultaneously and reliably with the largest possible rate, and at the same time, deliver the minimum required powers to the receivers: $\text{tr}(\mathbb{E}[\mathbf{Z}\mathbf{Z}^T]) \geq E_1$, $\text{tr}(\mathbb{E}[\mathbf{Y}\mathbf{Y}^T]) \geq E_2$. The problem without the receiver-side constraints is solved by Weingarten et. al. [11]. The rate region is achieved using DPC along with time sharing. We show in the following theorem that the DPC is optimal even after imposing the receiver-side power constraints.

Theorem 4 *The capacity region of a MIMO broadcast channel with a transmitter-side power constraint P and minimum receiver-side power constraints E_1, E_2 , $\mathcal{C}(E_1, E_2, P, \mathbf{H}, \mathbf{G})$, is given by the DPC region, which is the convex hull of the union of two regions \mathcal{R}_1^{DPC} and \mathcal{R}_2^{DPC} , corresponding to the two orders of encoding, given as:*

$$\begin{aligned} \mathcal{R}_1^{DPC} &= \left\{ (R_1, R_2) : R_1 \leq \frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}_1\mathbf{H}^T|, \quad R_2 \leq \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T|}{|\mathbf{I} + \mathbf{G}\mathbf{Q}_1\mathbf{G}^T|} \right\} \\ \mathcal{R}_2^{DPC} &= \left\{ (R_1, R_2) : R_1 \leq \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T|}{|\mathbf{I} + \mathbf{H}\mathbf{Q}_2\mathbf{H}^T|}, \quad R_2 \leq \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}_2\mathbf{G}^T| \right\} \end{aligned} \quad (95)$$

both of which subject to

$$\text{tr}(\mathbf{Q}_1 + \mathbf{Q}_2) \leq P, \quad \text{tr}(\mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E}_1, \quad \text{tr}(\mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T) \geq \tilde{E}_2 \quad (96)$$

Proof: We consider, without loss of generality, the region of rates achieved by \mathcal{R}_1^{DPC} . We first note that, due to the presence of the minimum receiver-side power constraints, we need to consider a double-sided correlation matrix constraint $\mathbf{S}_1 \preceq \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2$, for any fixed $\mathbf{S}_1, \mathbf{S}_2$ in $\mathcal{S}_{PE_1E_2}$ in (84). Following the original channel enhancement proof of the aligned MIMO (not necessarily degraded) BC (AMBC) in [11], it suffices to prove that under a double-sided correlation matrix constraint $\mathbf{S}_1 \preceq \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2$, there exists an enhanced aligned degraded BC (ADBC) such that for $\alpha_1 \leq \alpha_2$, noise covariances of the enhanced channel satisfy the covariance increment $\tilde{\mathbf{N}}_1 \preceq \tilde{\mathbf{N}}_2$ and supporting hyperplane preservation.

First, the achievable DPC rates in the aligned case with the encoding order in \mathcal{R}_1^{DPC} are

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \alpha_1 \cdot \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{N}_1|}{|\mathbf{N}_1|} + \alpha_2 \cdot \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_2|}{|\mathbf{Q}_1 + \mathbf{N}_2|} \\ \text{s.t.} \quad & \mathbf{Q}_1 + \mathbf{Q}_2 \succeq \mathbf{S}_1, \quad \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2 \end{aligned} \quad (97)$$

The Lagrangian for this problem is:

$$\begin{aligned} \mathcal{L} = & \alpha_1 \cdot \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{N}_1|}{|\mathbf{N}_1|} + \alpha_2 \cdot \frac{1}{2} \log \frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_2|}{|\mathbf{Q}_1 + \mathbf{N}_2|} + \text{tr}(\mathbf{Q}_1 \mathbf{M}_1) + \text{tr}(\mathbf{Q}_2 \mathbf{M}_2) \\ & + \text{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_1) \mathbf{M}_3) - \text{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_2) \mathbf{M}_4) \end{aligned} \quad (98)$$

The KKT optimality conditions for $\mathbf{Q}_1^*, \mathbf{Q}_2^*$ are:

$$\frac{\alpha_1}{2}(\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} + \frac{\alpha_2}{2}(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - \frac{\alpha_2}{2}(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_1 + \mathbf{M}_3 - \mathbf{M}_4 = \mathbf{0} \quad (99)$$

$$\frac{\alpha_2}{2}(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 + \mathbf{M}_3 - \mathbf{M}_4 = \mathbf{0} \quad (100)$$

and the complementary slackness conditions are as in (27)-(29). From (100) and (99), we have:

$$\frac{\alpha_1}{2}(\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 = \frac{\alpha_2}{2}(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 \quad (101)$$

Consequently, we construct the enhanced channels as:

$$\frac{\alpha_1}{2}(\mathbf{Q}_1^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 = \frac{\alpha_1}{2}(\mathbf{Q}_1^* + \tilde{\mathbf{N}}_1)^{-1} \quad (102)$$

$$\frac{\alpha_2}{2}(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 = \frac{\alpha_2}{2}(\mathbf{Q}_1^* + \tilde{\mathbf{N}}_2)^{-1} \quad (103)$$

Then, $\tilde{\mathbf{N}}_1 \preceq \mathbf{N}_1$ and $\tilde{\mathbf{N}}_2 \preceq \mathbf{N}_2$, and thus, the constructed channels are enhanced. We need show that the enhanced BC is degraded in favor of receiver 1. Since $\alpha_1 \leq \alpha_2$, from (101)-(103),

$$(\mathbf{Q}_1^* + \tilde{\mathbf{N}}_1)^{-1} = \frac{\alpha_2}{\alpha_1}(\mathbf{Q}_1^* + \tilde{\mathbf{N}}_2)^{-1} \succeq (\mathbf{Q}_1^* + \tilde{\mathbf{N}}_2)^{-1} \quad (104)$$

and hence $\tilde{\mathbf{N}}_1 \preceq \tilde{\mathbf{N}}_2$. Moreover, we have the rate preservation relation of receiver 1,

$$\frac{|\mathbf{Q}_1^* + \tilde{\mathbf{N}}_1|}{|\tilde{\mathbf{N}}_1|} = \frac{|\mathbf{Q}_1^* + \mathbf{N}_1|}{|\mathbf{N}_1|} \quad (105)$$

and the rate preservation for user 2 can be shown as:

$$(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \tilde{\mathbf{N}}_2)(\mathbf{Q}_1^* + \tilde{\mathbf{N}}_2)^{-1} = \mathbf{Q}_2^*(\mathbf{Q}_1^* + \tilde{\mathbf{N}}_2)^{-1} + \mathbf{I} \quad (106)$$

$$= \mathbf{Q}_2^*[(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \frac{2}{\alpha_2}\mathbf{M}_2] + \mathbf{I} \quad (107)$$

$$= \mathbf{Q}_2^*(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{I} \quad (108)$$

$$= (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} \quad (109)$$

leading to:

$$\frac{|\mathbf{Q}_1^* + \mathbf{Q}_2^* + \tilde{\mathbf{N}}_2|}{|\mathbf{Q}_1^* + \tilde{\mathbf{N}}_2|} = \frac{|\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{Q}_1^* + \mathbf{N}_2|} \quad (110)$$

Hence, we have an enhanced ADBC whose rate region is achieved by a Gaussian codebook and use full \mathbf{S}_2 [11]. Additionally, from (105) and (110), we conclude that the rate region of the original AMBC coincides with the optimal Gaussian rate region $\mathcal{R}^G(\mathbf{S}_2, \tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2)$ of the enhanced ADBC. To complete the proof, we need to show that the supporting hyperplane $\{(R_1, R_2) : \alpha_1 R_1 + \alpha_2 R_2 = b\}$ is also a supporting hyperplane for the Gaussian rate region of the enhanced ADBC $\mathcal{R}^G(\mathbf{S}_2, \tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2)$, i.e., that $\sum_{i=1}^2 \alpha_i R_i^G(\mathbf{Q}_1, \mathbf{Q}_2, \tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2)$ is maximized by the \mathbf{Q}_i^* that solves the AMBC problem. The proof of this follows from [11]. ■

We note that the related work [34] considers a MISO BC with multiple receivers, where each receiver requires either data or energy, but not both. The energy-requiring users are satisfied by the transmission of pseudo-random signals, that are known to all receivers, which can be subtracted out for communication purposes with the information-requiring users. The information-requiring users are served with a DPC scheme, which is optimal in that case due to [11], as energy transfer does not interact with data transfer. The emphasis in [34] is the optimization of the system for this

transmission scheme. In our work, all users require both data and information simultaneously. We prove by developing a suitable channel enhancement method using double-sided correlation matrix constraints that DPC is optimal for this system.

D. Gaussian MIMO Broadcast Channel with Confidential messages Under Minimum Receiver-Side Power Constraints

In this section, we consider the MIMO BCCM where we transmit a message to each receiver secret from the other. In this setting, the transmitter is required to communicate messages reliably, securely and at the same time deliver minimum amounts of energy E_1 and E_2 to the receivers. The problem without receiver-side power constraints was solved in [20], and it was shown that secure DPC (S-DPC) attains the secrecy capacity region. We show in the following theorem that S-DPC is optimal in the presence of receiver-side power constraints as well.

Theorem 5 *The secrecy capacity region of a MIMO broadcast channel with a transmitter-side power constraint P and minimum receiver-side power constraints E_1, E_2 and with secrecy constraints, $\mathcal{C}(E_1, E_2, P, \mathbf{H}, \mathbf{G})$, is given by the S-DPC region,*

$$\begin{aligned}
 R_1 &\leq \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}_1\mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}_1\mathbf{G}^T| \\
 R_2 &\leq \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T|}{|\mathbf{I} + \mathbf{G}\mathbf{Q}_1\mathbf{G}^T|} - \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T|}{|\mathbf{I} + \mathbf{H}\mathbf{Q}_1\mathbf{H}^T|} \\
 \text{s.t. } &\text{tr}(\mathbf{Q}_1 + \mathbf{Q}_2) \leq P \\
 &\text{tr}(\mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E}_1, \quad \text{tr}(\mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T) \geq \tilde{E}_2
 \end{aligned} \tag{111}$$

This region is achieved by S-DPC (Gaussian double binning) using jointly Gaussian random variables $(\mathbf{V}_1, \mathbf{V}_2) \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}, \mathbf{Z})$ such that $\mathbf{V}_1 = \mathbf{U}_1 + \mathbf{F}\mathbf{U}_2$, $\mathbf{V}_2 = \mathbf{U}_2$, $\mathbf{X} = \mathbf{U}_1 + \mathbf{U}_2$, where $\mathbf{U}_1 \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_1)$, $\mathbf{U}_2 \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_2)$ are independent and $\mathbf{F} = \mathbf{Q}_1\mathbf{H}^T(\mathbf{I} + \mathbf{H}\mathbf{Q}_1\mathbf{H}^T)^{-1}\mathbf{H}$.

Proof: In this case also, we have a double-sided correlation matrix constraint $\mathbf{S}_1 \preceq \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2$, where $\mathbf{S}_1, \mathbf{S}_2$ in $\mathcal{S}_{PE_1E_2}$ in (84). From Lemma 4, we know that, to have a positive secrecy rate at receiver 2, we must use the full correlation matrix \mathbf{S}_2 , i.e., $\mathbf{Q}_1 + \mathbf{Q}_2 = \mathbf{S}_2$. Since the outer optimization problem chooses \mathbf{S}_2 from the set $\mathcal{S}_{PE_1E_2}$, and \mathbf{X} has the covariance $\mathbf{Q} = \mathbf{Q}_1 + \mathbf{Q}_2$, the receiver-side power constraints are satisfied. The achievability of the corner point follows from [20] by using the double binning scheme presented in [35].

We next need to show that the achievable scheme matches the converse. For receiver 2: From Theorem 1, noticing that \mathbf{G} in this case corresponds to the main channel and \mathbf{H} corresponds to the eavesdropper channel, the achievable rate $R_{2,\max}$ in (111) is equal to the secrecy capacity $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{G}, \mathbf{H})$ in (18) proving the converse. For receiver 1: The achievable rate $R_{1,\max}$ in (111) is the same as the secrecy capacity $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ in (11) except for the correlation constraint $\mathbf{S}_1 \preceq \mathbf{Q}_1 + \boldsymbol{\mu}\boldsymbol{\mu}^T \preceq \mathbf{S}_2$. Recall that, in Section IV-B, we proved the converse for arbitrary \mathbf{Q}_2 , not necessarily unit-rank. Therefore, using S-DPC encoding scheme induces the required extra covariance component \mathbf{Q}_2 that supports the receiver-side constraint. Moreover, we observe that

$$C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{G}, \mathbf{H}) = C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) + \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{G}\mathbf{S}_2\mathbf{G}^T|}{|\mathbf{I} + \mathbf{H}\mathbf{S}_2\mathbf{H}^T|} \quad (112)$$

This implies that \mathbf{Q}_1 maximizes the secrecy capacities of both users simultaneously. Consequently, the two users can receive the confidential messages at their respective maximum secrecy rates as individual wiretap channels, i.e., the secrecy rate region is rectangular under the $\mathbf{S}_1, \mathbf{S}_2$ correlation matrix constraints. Hence, the S-DPC scheme is optimal. ■

VI. PRACTICAL OPTIMIZATION APPROACHES

In this section, we provide several optimization approaches to evaluate the capacities under receiver-side power constraints stated in Theorems 1-5. Without loss of generality, we consider the case of a single minimum receiver-side power constraint in the wiretap channel in Theorem 1. This is one of the most challenging optimization problems among the results in Theorems 1-5, as the optimization problem in this case is not convex.

A. MISO Problem with Gaussian Mean-Based Coding Scheme

The MISO problem with Gaussian mean-based coding scheme can be exactly cast as a convex optimization problem by considering a linear fractional transformation (Charnes-Cooper transformation) [36] as follows:

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \frac{1}{2} \log(1 + \mathbf{h}^T \mathbf{Q}_1 \mathbf{h}) - \frac{1}{2} \log(1 + \mathbf{g}^T \mathbf{Q}_1 \mathbf{g}) \\ \text{s.t.} \quad & \text{tr}(\mathbf{Q}_1) + \text{tr}(\mathbf{Q}_2) \leq P, \quad \mathbf{g}^T (\mathbf{Q}_1 + \mathbf{Q}_2) \mathbf{g} \geq \tilde{E} \end{aligned} \quad (113)$$

The objective function is generally not concave. Considering the monotonicity of \log , the objective function can be replaced with the linear fractional objective function $\frac{1+\mathbf{h}^T\mathbf{Q}_1\mathbf{h}}{1+\mathbf{g}^T\mathbf{Q}_1\mathbf{g}}$. Following the linear fractional transformation [36] by multiplying by positive variable $t > 0$ and defining $\mathbf{Q}_1 = \tilde{\mathbf{Q}}_1/t$, $\mathbf{Q}_2 = \tilde{\mathbf{Q}}_2/t$, and fixing the resultant denominator as $t + \mathbf{g}^T\tilde{\mathbf{Q}}_1\mathbf{g} = 1$, we obtain the convex equivalent of the problem in (113) as

$$\begin{aligned} \max_{\tilde{\mathbf{Q}}_1, \tilde{\mathbf{Q}}_2 \succeq \mathbf{0}, t > 0} \quad & t + \mathbf{h}^T\tilde{\mathbf{Q}}_1\mathbf{h} \\ \text{s.t.} \quad & t + \mathbf{g}^T\tilde{\mathbf{Q}}_1\mathbf{g} = 1 \\ & \text{tr}(\tilde{\mathbf{Q}}_1) + \text{tr}(\tilde{\mathbf{Q}}_2) \leq tP, \quad \mathbf{h}^T(\tilde{\mathbf{Q}}_1 + \tilde{\mathbf{Q}}_2)\mathbf{h} \geq t\tilde{E} \end{aligned} \quad (114)$$

The optimal solution of (114) can be obtained efficiently using convex solvers, e.g., CVX.

B. MISO Problem with Gaussian Artificial Noise Based Coding Scheme

In this case, we cannot fully transform the problem to a convex form. However, we can apply similar techniques together with an extra step of line search [37] to solve the problem. The problem in this case is:

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \frac{1}{2} \log \left(1 + \frac{\mathbf{h}^T\mathbf{Q}_1\mathbf{h}}{1 + \mathbf{h}^T\mathbf{Q}_2\mathbf{h}} \right) - \underbrace{\frac{1}{2} \log \left(1 + \frac{\mathbf{g}^T\mathbf{Q}_1\mathbf{g}}{1 + \mathbf{g}^T\mathbf{Q}_2\mathbf{g}} \right)}_{\leq \beta} \\ \text{s.t.} \quad & \text{tr}(\mathbf{Q}_1) + \text{tr}(\mathbf{Q}_2) \leq P, \quad \mathbf{g}^T(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{g} \geq \tilde{E} \end{aligned} \quad (115)$$

Next, we upper bound the second term in the optimization problem by $\frac{1}{2} \log \beta$, where β is the line-search variable. This results in an extra constraint $\frac{\mathbf{g}^T\mathbf{Q}_1\mathbf{g}}{1+\mathbf{g}^T\mathbf{Q}_2\mathbf{g}} \leq \beta - 1$. We write the optimization problem by considering the monotonicity of \log and rearranging terms as:

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \frac{1 + \mathbf{h}^T(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{h}}{\beta(1 + \mathbf{h}^T\mathbf{Q}_2\mathbf{h})} \\ \text{s.t.} \quad & \mathbf{g}^T(\mathbf{Q}_1 - (\beta - 1)\mathbf{Q}_2)\mathbf{g} \leq \beta - 1 \\ & \text{tr}(\mathbf{Q}_1) + \text{tr}(\mathbf{Q}_2) \leq P, \quad \mathbf{g}^T(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{g} \geq \tilde{E} \end{aligned} \quad (116)$$

Now, by linear fractional transformation [36], we multiply (116) by $t > 0$, define $\mathbf{Q}_1 = \tilde{\mathbf{Q}}_1/t$, $\mathbf{Q}_2 = \tilde{\mathbf{Q}}_2/t$ and fix $\beta(t + \mathbf{h}^T\tilde{\mathbf{Q}}_2\mathbf{h}) = 1$. Note that using this transformation, the resultant problem is a convex problem for fixed β . Hence, iterating over β along its range $1 \leq \beta \leq$

$1 + P\|\mathbf{h}\|^2$, the problem becomes

$$\max_{\beta} \varphi(\beta), \quad \text{s.t.} \quad 1 \leq \beta \leq 1 + P\|\mathbf{h}\|^2 \quad (117)$$

which together with the following can be solved effectively

$$\begin{aligned} \varphi(\beta) = \max_{\tilde{\mathbf{Q}}_1, \tilde{\mathbf{Q}}_2 \succeq \mathbf{0}, t > 0} \quad & t + \mathbf{h}^T(\tilde{\mathbf{Q}}_1 + \tilde{\mathbf{Q}}_2)\mathbf{h} \\ \text{s.t.} \quad & \mathbf{g}^T(\tilde{\mathbf{Q}}_1 - (\beta - 1)\tilde{\mathbf{Q}}_2)\mathbf{g} \leq t(\beta - 1) \\ & \beta(t + \mathbf{h}^T\tilde{\mathbf{Q}}_2\mathbf{h}) = 1 \\ & \text{tr}(\tilde{\mathbf{Q}}_1) + \text{tr}(\tilde{\mathbf{Q}}_2) \leq tP, \quad \mathbf{g}^T(\tilde{\mathbf{Q}}_1 + \tilde{\mathbf{Q}}_2)\mathbf{g} \geq t\tilde{E} \end{aligned} \quad (118)$$

C. General MIMO Problem

For the general MIMO case, we cannot provide a direct convex optimization equivalent as in the MISO case even by adding a line search. This is due to the concavity of log-determinant functions, which result in difference of concave functions. To tackle the problem, we can approximate the objective function using sequential convex optimization techniques [38], [39]. The idea here is to approximate the second term in the objective function by its first order expansion. To show that, first, consider the objective function of the Gaussian coding with fixed mean $\frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}_1\mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}_1\mathbf{G}^T|$, which is equivalent to $\log |\mathbf{Q}_1 + \mathbf{N}_1| - \log |\mathbf{Q}_1 + \mathbf{N}_2|$. We approximate the second term with an affine function using the Taylor series expansion of the log det function around $\mathbf{Q}^{(k)}$, where k denotes the k th iteration:

$$\log |\mathbf{Q}_1 + \mathbf{N}_2| \cong \log |\mathbf{Q}_1^{(k)} + \mathbf{N}_2| + \text{tr}((\mathbf{Q}_1^{(k)} + \mathbf{N}_2)^{-1}(\mathbf{Q}_1 - \mathbf{Q}^{(k)})) \quad (119)$$

Since the constant terms do not affect the optimal solution, we can use

$$\log |\mathbf{Q}_1 + \mathbf{N}_2| \cong \text{tr}((\mathbf{Q}_1^{(k)} + \mathbf{N}_2)^{-1}\mathbf{Q}_1) \quad (120)$$

The optimization problem in the k th iteration is

$$\begin{aligned} \max_{\mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}} \quad & \log |\mathbf{Q}_1 + \mathbf{N}_1| - \text{tr}((\mathbf{Q}_1^{(k)} + \mathbf{N}_2)^{-1}\mathbf{Q}_1) \\ \text{s.t.} \quad & \text{tr}(\mathbf{Q}_1) + \text{tr}(\mathbf{Q}_2) \leq P, \quad \text{tr}(\mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E} \end{aligned} \quad (121)$$

which is a convex problem, and can be solved efficiently. We update $\mathbf{Q}_1^{(k)}, \mathbf{Q}_2^{(k)}$ by solving such convex optimization problems until convergence.

Finally, using similar ideas, we can perform linearization in the case of Gaussian with artificial noise coding scheme, where the corresponding optimization problem in the k th iteration is

$$\begin{aligned} \max_{\mathbf{Q}_2, \mathbf{S} \succeq \mathbf{0}} \quad & \log |\mathbf{S} + \mathbf{N}_1| + \log |\mathbf{Q}_2 + \mathbf{N}_2| - \text{tr}((\mathbf{Q}_2^{(k)} + \mathbf{N}_1)^{-1} \mathbf{Q}_2) - \text{tr}((\mathbf{S}^{(k)} + \mathbf{N}_2)^{-1} \mathbf{S}) \\ \text{s.t.} \quad & \text{tr}(\mathbf{S}) \leq P, \quad \text{tr}(\mathbf{G} \mathbf{S} \mathbf{G}^T) \geq \tilde{E} \end{aligned} \quad (122)$$

VII. NUMERICAL RESULTS

In this section, we present simple simulation results for the secrecy capacity of the MIMO wiretap channel with maximum transmitter-side power constraint and minimum receiver-side (eavesdropper-side) power constraint. In these simulations, the average transmit power at the transmitter is taken as $P = 10$ and the noise covariance is identity at both receivers.

Fig. 2 shows a secrecy capacity receiver-side power constraint region for a MISO 4-1-1 system, i.e, a system with 4 antennas at the transmitter and single antenna at both the legitimate receiver and the eavesdropper. The figure shows the optimality of the Gaussian signalling with a mean and Gaussian coding with Gaussian artificial noise coding schemes; in particular, the regions corresponding to the mean and artificial noise coding schemes are identical. Moreover, the secrecy rate region with receiver-side power region of the standard Gaussian coding scheme with no mean or no artificial noise is noticeably smaller than the optimal schemes. That is, the standard Gaussian signaling scheme is strictly sub-optimal for the case of receiver-side power constraints. In addition, we observe that, as the receiver-side power constraint is increased, the secrecy capacity decreases, i.e., there is a trade-off between the power that should be delivered to the eavesdropper's receiver and the confidentiality that can be provided to the legitimate receiver. This is because, when the receiver-side power constraint is increased, the problem becomes more confined and more power should be concentrated for the receiver-side power constraint, which decreases the set of signalling choices for the secrecy communications. Fig. 3 shows similar observations for the 2-2-2 MIMO wiretap system.

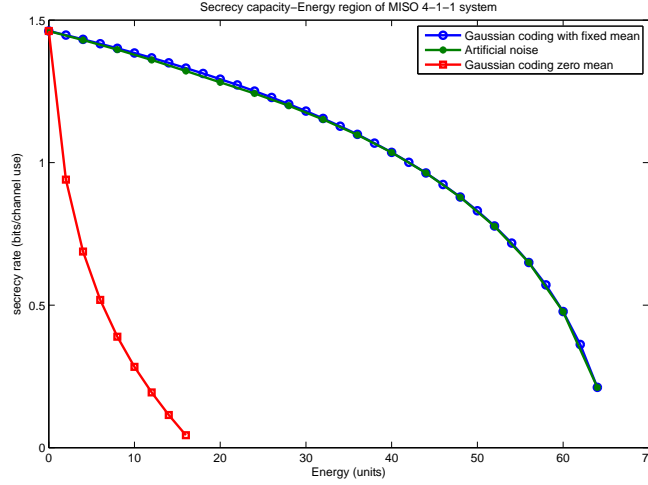


Fig. 2. Secrecy capacity receiver-side power constraint region for a 4-1-1 MISO wiretap channel.

VIII. CONCLUSIONS

We considered the MIMO wiretap channel with the usual transmitter-side maximum power constraint and an additional receiver-side minimum power constraint. For the converse, we first proved that the problem is equivalent to solving a secrecy capacity problem with a double-sided correlation matrix constraint on the channel input. We then extended the channel enhancement technique to our setting. For the achievability, we proposed two optimum schemes that achieve the converse rate: Gaussian signalling with a fixed mean and Gaussian signalling with Gaussian channel prefixing (artificial noise). This is the first instance of a problem where transmission with a mean or channel prefixing are strictly necessary for a MIMO wiretap channel under power constraints. The transmission scheme with a mean enables us to deliver the needed power to the receiver without creating interference to the legitimate receiver as it is a deterministic signal. On the other hand, the transmission scheme with Gaussian artificial noise, both jams the eavesdropper contributing to the secrecy as well as delivering the needed power to the receiver. We note that the optimal coding scheme for the MIMO wiretap channel under a transmitter-side power constraint only, which is Gaussian signalling with no channel prefixing or mean, is strictly sub-optimal when we impose a receiver-side power constraint, showing similar to the cases of [1], [2], that receiver-side power constraints may change the solution significantly and may introduce non-trivial trade-offs. We then extended our setting to the cases of minimum power constraints at both receivers in a wiretap channel; maximum receiver-side power constraints at both receivers in a wiretap channel; minimum receiver-side power constraints in a broadcast channel (i.e., no

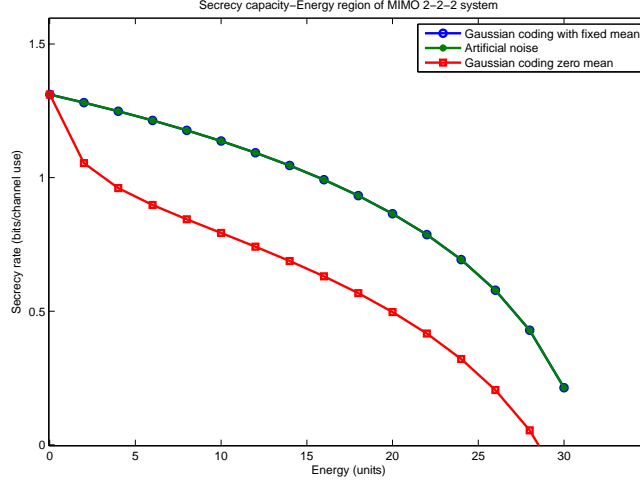


Fig. 3. Secrecy capacity receiver-side power constraint region for a 2-2-2 MIMO wiretap channel.

secrecy constraints); and minimum receiver-side power constraints in a broadcast channel with confidential messages (i.e., double-sided secrecy constraints).

APPENDIX

CONTINUITY OF THE CAPACITY FUNCTION

We prove our claim in Lemma 2 that $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ is a continuous function with respect to \mathbf{S}_2 . Although contiguity defined in [11], which is a weaker notion than continuity, suffices to prove Lemma 2, we prove continuity here. To prove this, we begin by writing the optimization problem in a general form as in [11, Appendix IV] by concatenating the rows of $\mathbf{Q}_1, \mathbf{Q}_2$ to form a vector $\mathbf{y} \in \mathbb{R}^{2t^2}$, where $t = \max\{N_t, N_r\}$. We denote the point-to-set map $\Omega(\mathbf{S}_2)$ to be a mapping from \mathbf{S}_2 to the power set of all subsets of the corresponding feasible set, i.e.,

$$\Omega(\mathbf{S}_2) = \{\text{row concatenation of } (\mathbf{Q}_1, \mathbf{Q}_2) : \mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}, \mathbf{S}_1 \preceq \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2\} \quad (123)$$

Denote $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ by $C(\mathbf{S}_2)$ for notational simplicity as we focus on the argument \mathbf{S}_2 here. From (11) with $\mathbf{Q}_2 = \boldsymbol{\mu}\boldsymbol{\mu}^T$, we write $C(\mathbf{S}_2)$ as

$$C(\mathbf{S}_2) = \max_{\mathbf{y} \in \Omega(\mathbf{S}_2)} f(\mathbf{y}) \quad (124)$$

where $f(\mathbf{y}) = \frac{1}{2} \log |\mathbf{I} + \mathbf{H}\mathbf{Q}_1\mathbf{H}^T| - \frac{1}{2} \log |\mathbf{I} + \mathbf{G}\mathbf{Q}_1\mathbf{G}^T|$. Note that in this case $f(\mathbf{y})$ depends only on the first t^2 elements of \mathbf{y} . Now, we use [40, Theorem 7], which states conditions on the continuity of the optimal value function in mathematical programming to prove the continuity

of $C(\mathbf{S}_2)$. In the sequel, we verify that all requirements of [40, Theorem 7] are satisfied.

Since the determinant of an $n \times n$ matrix \mathbf{A} can be written as $\det(\mathbf{A}) = \sum_{\sigma} \text{sgn}(\sigma) \prod_{i=1}^n a_{i\sigma(i)}$, where the sum is over all $n!$ permutations of $\{1, 2, \dots, n\}$, the determinant in this form is a polynomial in n^2 variables, and $\det(\mathbf{A})$ is continuous. Consequently, $f(\mathbf{y})$ is also continuous. $\Omega(\mathbf{S}_2)$ consists of linear matrix inequalities, hence it is a continuous point-to-set map. Furthermore, $\Omega(\mathbf{S}_2)$ is uniformly compact because for any sequence $\mathbf{S}_2^{(i)}$ in the neighborhood of \mathbf{S}_2 , i.e., the metric distance $d(\mathbf{S}_2^{(i)}, \mathbf{S}_2) = \text{tr} \left((\mathbf{S}_2^{(i)} - \mathbf{S}_2)(\mathbf{S}_2^{(i)} - \mathbf{S}_2)^T \right) \leq \delta^2$ for some finite $\delta > 0$, one can find $k_i = \max \lambda(\mathbf{S}_2^{(i)})$ where $\lambda(\mathbf{S}_2^{(i)})$ is an eigenvalue of matrix $\mathbf{S}_2^{(i)}$ such that

$$\Omega(\mathbf{S}_2^{(i)}) \subseteq \mathcal{Y} = \{\text{row concatenation of } (\mathbf{Q}_1, \mathbf{Q}_2) : \mathbf{Q}_1, \mathbf{Q}_2 \succeq \mathbf{0}, \text{tr}(\mathbf{Q}_1 + \mathbf{Q}_2) \leq k\} \quad (125)$$

where $k = \max_i k_i \leq P + \delta$, where P is the power constraint imposed on \mathcal{S}_{PE} . Since \mathcal{Y} is compact and contains $\bigcup_i \Omega(\mathbf{S}_2^{(i)})$, $\Omega(\mathbf{S}_2)$ is uniformly compact. Hence, the requirements of [40, Theorem 7] are satisfied and $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ is continuous with respect to \mathbf{S}_2 .

REFERENCES

- [1] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. on Inform. Theory*, vol. 53, no. 2, pp. 471–487, February 2007.
- [2] L. R. Varshney, "Transporting information and energy simultaneously," in *IEEE ISIT*, July 2008.
- [3] J. G. Smith, "The information capacity of amplitude and variance-constrained scalar Gaussian channels," *Information and Control*, vol. 18, pp. 203–219, April 1971.
- [4] A. D. Wyner, "The wire-tap channel," *The Bell System Tech. Jour.*, vol. 54, no. 8, pp. 1355–1387, January 1975.
- [5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [6] S. K. Leung-Yan-Cheung and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Inform. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
- [7] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. on Inform. Theory*, vol. 55, no. 9, pp. 4033–4039, September 2009.
- [8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas – Part II: The MIMOME wiretap channel," *IEEE Trans. on Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, November 2010.
- [9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. on Inform. Theory*, vol. 57, no. 8, pp. 4961–4972, August 2011.
- [10] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. on Inform. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.
- [11] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. on Inform. Theory*, vol. 52, no. 9, pp. 3936–3964, September 2006.
- [12] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. on Wireless Comm.*, vol. 7, no. 6, pp. 2180–2189, June 2008.
- [13] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. on Inform. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

- [14] Z. Li, R. D. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. on Wireless Comm.*, vol. 9, no. 9, pp. 2792–2799, September 2010.
- [15] Z. Rezk, A. Khisti, and M. S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. on Comm.*, vol. 62, no. 10, pp. 3652–3664, October 2014.
- [16] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. on Vehicular Tech.*, vol. 59, no. 8, pp. 3831–3842, October 2010.
- [17] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. on Signal Proc.*, vol. 59, no. 1, pp. 351–361, January 2011.
- [18] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. on Wireless Comm.*, vol. 10, no. 3, pp. 901–915, March 2011.
- [19] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. on Inform. Theory.*, vol. 60, no. 6, pp. 3359–3378, June 2014.
- [20] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory.*, vol. 56, no. 9, pp. 4215–4227, September 2010.
- [21] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. on Signal Proc.*, vol. 62, no. 7, pp. 1850–1863, April 2014.
- [22] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. on Wireless Comm.*, vol. 13, no. 8, pp. 4599–4615, August 2014.
- [23] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K.-K. Wong, and H. Zhu, "Achievable ergodic secrecy rate for MIMO SWIPT wiretap channels," in *IEEE ICC*, June 2015.
- [24] —, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. on Info. Forensics and Security*, vol. 11, no. 1, pp. 74–85, January 2016.
- [25] T. M. Cover and J. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2012.
- [26] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.
- [27] A. E. Gamal and Y.-H. Kim, *Network information theory*. Cambridge university press, 2011.
- [28] R. Gallager, *Information theory and reliable communication*. New York: Wiley, 1968.
- [29] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. on Info. Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.
- [30] V. Bryant, *Metric Spaces: Iteration and Application*. Cambridge University Press, 1985.
- [31] H. L. Royden and P. Fitzpatrick, *Real Analysis*. Prentice Hall, 2010.
- [32] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge University Press, 2012.
- [33] A. R. Meenakshi and C. Rajian, "On a product of positive semidefinite matrices," *Linear Algebra and its Applications*, vol. 295, no. 1, pp. 3–6, July 1999.
- [34] S. Luo, J. Xu, T. J. Lim, and R. Zhang, "Capacity region of MISO broadcast channel with SWIPT," in *IEEE ICC*, June 2015.
- [35] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. on Inform. Theory.*, vol. 54, no. 6, pp. 2493–2507, June 2008.
- [36] S. P. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.
- [37] J. Li and A. Petropulu, "Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels," in *IEEE ICASSP*, March 2010.
- [38] T. Wang and L. Vandendorpe, "Successive convex approximation based methods for dynamic spectrum management," in *IEEE ICC*, June 2012, pp. 4061–4065.
- [39] T. Lipp and S. P. Boyd, "Variations and extensions of the convex-concave procedure," 2014, available at http://web.stanford.edu/~boyd/papers/pdf/cvx_ccv.pdf.
- [40] W. Hogan, "Point-to-set maps in mathematical programming," *Siam Review*, vol. 15, no. 3, pp. 591–603, 1973.